IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF MISSISSIPPI
NORTHERN DIVISION

STEVEN SANDERS, *individually and on behalf of others similarly situated,* **Plaintiff,** **v.** **YAZOO VALLEY ELECTRIC POWER ASSOCIATION,** **Defendant.**	**CLASS ACTION** **CASE NO.** 3:25-cv-112-DPJ-ASH **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Steven Sanders ("Plaintiff"), by and through undersigned counsel, on behalf of himself and all others similarly situated, alleges the following Class Action Complaint (the "Action") against Yazoo Valley Electric Power Association ("Yazoo" or "Defendant") upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of counsel as follows:

I. SUMMARY

1. Plaintiff brings this Action on behalf of himself and all other similarly situated victims as a result of a recent cyberattack and data breach involving his personally identifiable information suffered by Yazoo.

2. On or about August 26, 2024, an unknown and unauthorized criminal actor gained access to Defendant's network and exfiltrated, at a minimum, names and Social Security Numbers. ("PII")[1].

[1] Notice of Data Breach, attached hereto as **Exhibit A.**

3. In the Notice of Data Breach letter, Yazoo sent to Plaintiff and Class Members on or around January 30, 2025, Yazoo explains[2]:

> **What Happened?**
> On or about August 26, 2024, we became aware of suspicious activity on our network… A thorough investigation determined that an unauthorized actor accessed certain files on our network. We then conducted a thorough review of the potentially impacted data to determine the types of information contained therein and to whom the information related. On October 24, 2024, we completed our review and determined that a limited amount of personal information may have been accessed by and unauthorized party in connection with this incident…
>
> **What Information Was Involved?**
> The potentially accessed information may have included your name in combination with Social Security number.[3]

4. To be clear – there are numerous issues with Yazoo's Data Breach, but the deficiencies in the Data Breach notification letter exacerbate the circumstances for victims of the Data Breach: (1) Yazoo waited nearly six months to notify Plaintiff and Class members of the Data Breach; (2) Yazoo fails to state whether it was able to contain or end the cybersecurity threat, leaving victims to fear whether the PII that Yazoo continues to maintain is secure; and (3) Yazoo fails to state how the breach itself occurred. All of this information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity of information compromised in this specific breach.

5. As a result of the Data Breach, Plaintiff and Class Members suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, loss of the benefit of their bargain, out-of-pocket expenses, loss of value of their time reasonably

[2] *Id.*
[3] Exhibit A.

incurred to remedy or mitigate the effects of the attack, invasion of their privacy and the loss of, and diminution in, value of their personal information.

6. In addition, Plaintiff's and Class Members' sensitive PII —which was entrusted to Defendant — was compromised and unlawfully accessed due to the Data Breach. This information, while compromised and taken by unauthorized third parties, remains also in the possession of Defendant, and without additional safeguards and independent review and oversight, remains vulnerable to future cyberattacks and theft.

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect victims' PII.

8. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party.

9. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant's computer network in a condition vulnerable to cyberattacks.

10. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant and entities like it, and Defendant was thus on notice that failing to take steps necessary to secure the PII against those risks left that property in a dangerous condition and vulnerable to theft. Defendant was further on notice of the severe consequences that would result to Plaintiff and Class Members from its failure to safeguard their PII.

11. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff and Class members' PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members prompt notice of the Data Breach.

12. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the PII. Had Defendant properly monitored its computer network and systems, it would have discovered the intrusion sooner, as opposed to letting cyberthieves roam freely in Defendant's IT network for months or even years.

13. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves. This present risk will continue for their respective lifetimes.

14. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

15. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

16. Plaintiff and Class Members will incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach.

18. Plaintiff seeks remedies including, but not limited to, actual damages, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

19. Plaintiff also seeks injunctive and equitable relief to prevent future injury on behalf of himself and the putative Class.

II. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is purportedly over 22,000, and at least one Class member is a citizen of a state that is diverse from Defendant's citizenship.[4] Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

21. This Court has personal jurisdiction over Defendant Yazoo Valley Electric Power Association because its principal place of business is in Mississippi, and it does a significant amount of business in Mississippi.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant has its principal place of business located in this District, and a substantial part of the events giving rise to this action occurred in this District.

[4] *See https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/93c8c3c5-1c8d-47bc-bf45-aefb701811f9.html*

III. PARTIES

Plaintiff Steven Sanders

23. Plaintiff Steven Sanders is an individual citizen of Mississippi and received a Notice of Data Breach letter from Defendant on or around January 30, 2024. Plaintiff Dawson's data was exposed because he is a customer of Yazoo.

Defendant Yazoo

24. Defendant Yazoo Valley Electric Power Association is a Mississippi electric power association with its principal place of business located in Yazoo City, Mississippi. Defendant provides electricity services throughout numerous counties in Mississippi.

IV. FACTUAL ALLEGATIONS

Defendant's Business

25. According to Defendant Yazoo's website:

> Yazoo Valley Electric is a rural electric power association serving parts of six counties in Mississippi. We are dedicated to providing safe, reliable electric power to the members who own the system we build and maintain. [5]

26. Defendant collects personally identifiable information in the course of doing business. This personally identifiable information includes the PII which was compromised in the Data Breach alleged herein.

27. Prior to receiving services from Yazoo, Plaintiff and Class Members were required to and did in fact turn over their PII.

28. Upon information and belief, Defendant promises to maintain the confidentiality of Plaintiff's and Class Members' Private Information to ensure compliance with federal and state

[5] https://www.yazoovalley.com/

laws and regulations, and not to use or disclose Plaintiff's and Class Members' Private Information for non-essential purposes.

29. As a condition of receiving services from Yazoo, Yazoo requires that Plaintiff and Class Members entrust it with highly sensitive personal information.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

31. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members would not have entrusted Defendant with their Private Information had they known that Defendant would fail to implement industry standard protections for that sensitive information.

32. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Attack and Data Breach

33. On or about January 30, 2024, Defendant informed Plaintiff and the Class Members that their PII had been compromised via the Notice of Data Breach letter.

34. The personally identifiable information that was compromised includes, but is not limited to name and Social Security number.

35. Due to Defendant's inadequate security measures, Plaintiff and the Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

36. Upon information and belief, the PII was not encrypted prior to the data breach.

37. Upon information and belief, the cyberattack was targeted at Defendant as a company that collects and maintains valuable personal and financial data from its many current and former customers, including Plaintiff and Class Members.

38. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and Class Members.

39. Defendant had obligations to keep Plaintiff's and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

40. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach Was Foreseeable and the Defendant Was Aware of Its Risk

41. It is well known that PII, including names in particular are invaluable commodities and a frequent target of hackers.

42. In 2023, a record 3,205 data breaches occurred in the United States, resulting in about 349,221,481 sensitive records being exposed, a greater than 100% increase from 2019.[6]

43. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

---

[6] ITRC (Identity Theft Resource Center), *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/publication/2023-data-breach-report/ (last accessed December 9, 2024).

44. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), and, in light of the recent data breaches Wells Fargo has suffered, Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

45. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so that they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

46. Despite the prevalence of public announcements of data breach and data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

47. Data breaches are not only foreseeable but are also preventable. In *Data Breach and Encryption Handbook*, author Lucy Thompson states the following: "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[7]

48. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures… Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[8]

---

[7] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[8] *Id* at 2

49. The FTC has developed guides for businesses that stress the importance of employing sufficient data security measures. The FTC considers data security a business-decision, and informs companies that they should view it in the same way.

50. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. [9]

Defendant Had a Duty to Plaintiff and Class Members to Secure Private Information

51. Defendant is prohibited by the Federal Trade Commission Act ("FTCA") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

52. Additionally, Defendant is also required to maintain appropriate data security by various states' laws and regulations.

53. At all relevant times, Defendant had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably

[9] ***P****rotecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

to prevent foreseeable harm to Plaintiff and Class Members, and to *promptly* notify Plaintiff and Class Members when Defendant became aware that their PII may have been compromised.

54. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class relied on Defendant to secure their PII when they entrusted Defendant with the information required to receive services from Yazoo.

55. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

56. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

57. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[10] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[11]

58. The ramifications of Defendant's failure to keep PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of Personally Identifiable Information

59. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market

[10] 17 C.F.R. § 248.201 (2013).
[11] *Id*.
[12] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed December 9, 2024).

value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[13]

60. As a growing number of federal courts have begun to recognize the loss of value of PII as a viable damages theory, the sale of PII from data breaches, as in the Data Breach alleged herein, is particularly harmful to data breach victims – especially when it takes place on the dark web.

61. The dark net is an unindexed layer of the internet that requires special software or authentication to access.[14] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[15] This prevents dark web marketplaces from being easily identifiable to authorities or those not in the know.

62. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.[16] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address.

---

[13] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, *available at*: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed December 9, 2024).

[14] *What Is the Dark Web?,* Experian, *available at* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last accessed December 9, 2024).

[15] *Id.*

[16] *What is the Dark Web?* – Microsoft 365, *available at* https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last accessed December 9, 2024).

Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth and medical information.[17] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others." [18]

63. Plaintiff and Class Members' PII is a valuable commodity, a market exists for Plaintiff and Class Members' PII (which is why the Data Breach was perpetrated in the first place), and Plaintiff and Class Members' PII is being likely being sold by hackers on the dark web (as that is the *modus operandi* of data thieves) – as a result, Plaintiff and Class Members have lost the value of their PII, which is sufficient to plausibly allege injury arising from a data breach.

64. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[19] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[2021] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[22]

65. The PII stolen in this specific Data Breach was particularly harmful.

66. PII can be used to distinguish, identify, or trace an individual's identity, such as

---

[17] *Id.*; *What Is the Dark Web?,* Experian, *available at* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/(last accessed December 9, 2024).

[18] *What is the Dark Web?* – Microsoft 365, *available at* https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last accessed December 9, 2024).

[19] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed December 9, 2024).

[20] https://datacoup.com/ (last accessed December 9, 2024).

[21] https://digi.me/about-us (last accessed December 9, 2024).

[22] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed December 9, 2024).

their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[23]

67. Given the nature of Defendant's Data Breach, as well as the unreasonable delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII can easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

68. To date, Defendant has offered its victims *only one year* of identity monitoring services. The offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here, as evident by Defendant's encouragement to take additional steps to mediate harm in its Notice letter.[24]

69. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures.

Plaintiff's Experience

70. Plaintiff was required to provide and did provide his PII to Defendant as a condition of receiving services from Yazoo.

71. To date, Defendant has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach particularly given the fact that Plaintiff's PII has already been "impacted" in the Data Breach and likely been made available on the dark web to anyone wishing to purchase it.

72. Nor has Defendant compensated Plaintiff and Class Members for the time they will

[23] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.
[24] *See Notice* ("What You Can Do")

spend monitoring their accounts, placing credit freezes and fraud alerts, changing online passwords and other actions.

73. Plaintiff and Class Members have been further damaged by the compromise of their PII in the Data Breach which was "impacted" and is in the hands of cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the PII.

74. Plaintiff typically takes measures to protect his PII and is very careful about sharing his PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

75. Plaintiff stores any documents containing his PII in a safe and secure location, and she diligently chooses unique usernames and passwords for his online accounts.

76. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. In response to the Data Breach, Plaintiff has spent significant time monitoring his accounts and credit score, changing his online account passwords and verifying the legitimacy of the Notice and researching the Data Breach. This is time that was lost and unproductive and took away from other activities and duties.

77. Specifically, since the date of the breach Plaintiff has spent hours taking action to mitigate the harm he has suffered. Plaintiff (1) has spent, and continues to spend, considerable time and effort actively monitoring his accounts and credit; and (2) he has lost sleep due to the stress and anxiety she now suffers from the fear of his PII being exposed, misused and sold on the black market.

78. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII — a form of intangible property that she entrusted to Defendant for the purpose of

receiving services from Yazoo, which was compromised in and as a result of the Data Breach.

79. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially after his information was used multiple times by unauthorized individuals.

80. Plaintiff suffered emotional distress and increased stress and anxiety as a result of the Data Breach because of the actions he has been forced to undertake, the loss of control over his most intimate information, and the fact that he must remain vigilant for the remainder of his life.

81. Plaintiff has suffered imminent and impending injury arising from not only the increased risk, but also the existence of fraud, identity theft, and likely misuse resulting from his PII being placed in the hands of criminals.

82. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff as a condition of receiving services from Yazoo. Plaintiff, however, would not have entrusted his PII to Defendant had she known that it would fail to maintain adequate data security. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

83. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ACTION ALLEGATIONS

84. Plaintiff brings this suit on behalf of himself and a class of similarly situated individuals under Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, which is preliminarily defined as:

> All persons Defendant has identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").

85. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

86. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. It is reported that over 20,000 individuals have been affected by this breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

87. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

i. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

iv. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

v. Whether Defendant owed a duty to Class Members to safeguard their PII;

vi. Whether Defendant breached its duty to Class Members to safeguard their PII;

vii. Whether computer hackers obtained Class Members' PII in the Data Breach;

viii. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

ix. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

x. Whether Defendant's conduct was negligent; and;

xi. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

88. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

89. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

90. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the

same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

91. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

92. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

93. Likewise, particular issues under Federal Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

xii. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

xiii. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

xiv. Whether Defendant's failure to institute adequate protective security measures amounted to negligence; and

xv. Whether Defendant failed to take commercially reasonable steps to safeguard PII,

94. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

95. Plaintiff hereby repeats and realleges paragraphs 1 though 94 of this Complaint and incorporates them by reference herein.

96. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII for pecuniary gain, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

97. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

98. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed. The

harm that Plaintiff and Class Members experienced was within the zone of foreseeable harm known to Defendant.

99. Defendant's duty to use reasonable security measures arose as a result of the relationship that existed between each Defendant and Plaintiff and the Class. That relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a mandatory step in receiving services from Yazoo. While this relationship exists independent from any contract, it is recognized by Defendant's privacy practices, as well as applicable laws and regulations. Specifically, Defendant actively solicited and gathered PII as part of its business and was solely responsible for and in the position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a resulting data breach.

100. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

101. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices and the frequency of data breaches in general.

102. Defendant also had a common law duty to prevent foreseeable harm to others. Plaintiff and the Class were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems. It was foreseeable that Plaintiff and Class members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

103. Defendant's conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff's and the Class members' PII, including basic encryption techniques available to Defendant.

104. Plaintiff and the Class had and have no ability to protect their PII that was in, and remains in, Defendant's possession.

105. Defendant was in a position to effectively protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

106. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

107. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within Defendant's possession.

108. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

109. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

110. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

111. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), Defendant had a separate and independent duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

112. The FTCA is intended, in part, to protect individuals whose PII is maintained by another and who are unable to safeguard their information as they cannot exercise control or direction over the data security practices.

113. Plaintiff and the members of the Class are within the class of persons that the FTCA was intended to protect as their PII was collected and maintained by Defendant and they were unable to exercise control over Defendant's data security practices.

114. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against.

115. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the members of the Class.

116. Defendant breached its duties to Plaintiff and the members of the Class under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

117. Had Plaintiff and the members of the Class known that Defendant would not adequately protect their Private Information, Plaintiff and the members of the Class would not have entrusted Defendant with their Private Information.

118. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

119. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the members of the Class, they would not have been injured.

120. The injury and harm suffered by Plaintiff and the members of the Class was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet their duties, and that Defendant's breach would cause Plaintiff and the members of the Class to experience the foreseeable harms associated with the exposure of their Private Information.

121. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to control how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to

undertake appropriate and adequate measures to protect the PII in their continued possession; (vii) lost benefit of the bargain; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

122. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

123. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

124. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class are now at an increased risk of identity theft or fraud.

125. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff is entitled to and demands actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

126. Plaintiff hereby repeats and realleges paragraphs 1 though 94 of this Complaint and incorporates them by reference herein.

127. Plaintiff and the Class entrusted their PII to Defendant as a condition of receiving services from Yazoo. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen, as evidenced by the representations in its privacy policies.[25]

128. At the time Defendant acquired the PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

129. Implicit in the agreements between Plaintiff and Class Members and Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

130. Plaintiff and the Class would not have entrusted their PII to Defendant had they known that Defendant would make the PII internet-accessible, not encrypt sensitive data elements, and not delete the PII that Defendant no longer had a reasonable need to maintain it.

[25] *See https://www.yazoovalley.com/index.php/aboutus/#:~:text=We%20never%20sell%2C%20rent%2C%20lease, website%20will%20be%20kept%20confidential.&ttex=We%20are%20committed%20to%20ensuring%20the%20security%20of%20your%20personal%20informatiin.* ("The following privacy policy is intended to protect and secure the personally identifiable information[] you provides to our organization… We are committed to ensuring the security of your personal information.")

131. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

132. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

133. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; lost benefit of the bargain; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

134. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT III
INVASION OF PRIVACY – INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

135. Plaintiff hereby repeats and realleges paragraphs 1 though 94 of this Complaint and incorporates them by reference herein.

136. Plaintiff and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored and maintained by Defendant, and they are entitled to the

reasonable and adequate protection of their PII against foreseeable unauthorized access, as occurred with the Data Breach.

137. Plaintiff and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

138. Defendant intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party. Defendant's acts and omissions giving rise to the Data Breach were intentional in that the decisions to implement lax security and failure to timely notice Plaintiff and the Class were undertaken willfully and intentionally.

139. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

140. This invasion of privacy resulted from Defendant's intentional failure to properly secure and maintain Plaintiff's and Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded and private data.

141. Plaintiff's and Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with

safeguarding it. Further, the public has no legitimate concern in Plaintiff's and Class Members' PII, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

142. The disclosure of Plaintiff's and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

143. Defendant's willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiff's and Class Members' sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

144. The unauthorized access, exfiltration, and disclosure of Plaintiff's and Class Members' PII was without their consent, and in violation of various statutes, regulations and other laws.

145. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT IV
UNJUST ENRICHMENT/QUASI CONTRACT
(On Behalf of Plaintiff and the Class)

146. Plaintiff hereby repeats and realleges paragraphs 1 though 94 of this Complaint and incorporates them by reference herein.

147. This Count is brought in the alternative to Count II, Breach of Implied Contract.

148. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII. In so conferring this benefit, Plaintiff and Class

Members understood that part of the benefit Defendant derived from the PII would be applied to data security efforts to safeguard the PII.

149. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

150. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

151. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

152. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

153. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant or pay for Defendant's services.

154. Plaintiff and Class Members have no adequate remedy at law.

155. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended

and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

156. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

157. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class defined herein, prays for judgment as against Defendant as follows:

a.) For an Order certifying this action as a Class action and appointing Plaintiff and his counsel to represent the Class;

b.) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c.) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Breach;

d.) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e.) Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class;

f.) For an award of actual damages, compensatory damages, statutory damages and statutory penalties, in an amount to be determined, as allowable by law;

g.) For an award of punitive damages, as allowable by law;

h.) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i.) Pre- and post-judgment interest on any amounts awarded and,

j.) All such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury.

DATED: February 13, 2025

Respectfully submitted,

/s/ John F. Hawkins
John F. Hawkins

OF COUNSEL:

John F. Hawkins, Esq. (MS)
HAWKINS LAW, P.C.
226 North President Street (39201)
Post Office Box 24627
Jackson, Mississippi 39225-4627
Telephone: (601) 969-9692
Facsimile: (601) 914-3580
john@hgattorneys.com

SHAMIS & GENTILE P.A.
Andrew J. Shamis, Esq.*
Leanna A. Loginov, Esq.*
ashamis@shamisgentile.com
14 NE 1st Ave., Suite 705
Miami, Florida 33132
Tel: (305) 479-2299
**Pro hac vice forthcoming*

Attorneys for Plaintiff and the Class